PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to ensure that access to servers, workstations and other computer systems containing Electronic Protected Health Information (ePHI) is appropriately secured.

REVISION HISTORY

Reviewed: 01/01/2022.
Next Review: 01/01/2023.

DEFINITIONS

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of the MDHHS to implement a mechanism to log, document and where necessary create a system generated alert for all atypical activities related to login attempts on each system containing medium and high risk ePHI.

PROCEDURE

Department of Information Technology (DTMB)

It is the responsibility of DTMB to:

- Implement a mechanism to log, document and where necessary create a system generated alert for all atypical activities related to login attempts on each system containing medium and high risk ePHI.

- Report more than one active session on different machines and session activity outside the hours of 6 AM to 9 PM.
- Wherever reasonable, block a workforce member's login after three consecutive unsuccessful attempts.
- Report all login attempts of a suspicious nature, such as continuous attempts immediately to the HIPAA security office. All alerts must be automatically generated based on certain criteria established by MDHHS.

Workforce Member

Workforce members must change passwords when prompted upon login attempt. Passwords expire between 60 and 90 calendar days regardless of activity, depending on the system or application.

Division Director or Section Supervisor/Manager

A division director or section supervisor/managers must:

- Review login activity reports and logs on a periodic basis.
- Monitor system access and activity of all workforce members

REFERENCES

45 CFR 164.308(a)(5)

CONTACT

For more information regarding this policy and procedure, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.